F4

MOBILE EQUIPMENT, FINGERPRINT AUTHENTICATING METHOD FOR MOBILE EQUIPMENT AND RECORDING MEDIUM WITH FINGERPRINT AUTHENTICATING PROGRAM FOR MOBILE EQUIPMENT RECORDED THEREON

Publication number: JP2001358828
Publication date: 2001-12-26
Inventor: OKUNO MASAHIKO
Applicant: OKUNO MASAHIKO
Classification:
- international: ***G06F1/00; G06F15/00; G06F21/20; G09C1/00; H04L9/32; H04M1/67; H04Q7/38;*** **G06F1/00; G06F15/00; G06F21/20; G09C1/00; H04L9/32; H04M1/66; H04Q7/38;** (IPC1-7): H04M1/67; G06F1/00; G06F15/00; G09C1/00; H04L9/32; H04Q7/38
- European:
Application number: JP20000213459 20000610
Priority number(s): JP20000213459 20000610

Abstract of **JP2001358828**

PROBLEM TO BE SOLVED: To provide mobile equipment capable of accurately confirming an individual and securing further safety by recognizing a user. SOLUTION: This mobile equipment is provided with a fingerprint recording medium for recording fingerprint data and a fingerprint recording medium reader for reading the fingerprint data from the fingerprint recording medium. The equipment is further provided with a fingerprint reader for reading fingerprint images and generating the fingerprint data and an authentication controller for transmitting the fingerprint data to a fingerprint authenticating server and receiving the judgment result of individual confirmation performed by the fingerprint authenticating server. When the individual is confirmed by them, the control for enabling the various kinds of operations as the mobile equipment is performed. Also, after authentication confirmation, the control for recording and reading the authentication data of received permits and tickets, etc., by using an authentication data recording medium is performed. Also, an IC card is provided with the fingerprint reader for reading the fingerprint images and generating the fingerprint data.

F4

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－358828
（P2001－358828A）
(43)公開日　平成13年12月26日(2001.12.26)

(51)Int.Cl.'		識別記号	FI			テーマコード'(参考)
H04M	1/67		H04M	1/67		5B085
G06F	1/00	370	G06F	1/00	370E	5J104
	15/00	330		15/00	330F	5K027
G09C	1/00	660	G09C	1/00	660B	5K067
H04Q	7/38		H04B	7/26	109R	

審査請求　未請求　請求項の数23　書面　（全 12 頁）　最終頁に続く

(21)出願番号　特願2000－213459(P2000－213459)

(22)出願日　平成12年６月10日(2000.6.10)

(71)出願人　396016401
奥野　昌彦
東京都品川区東五反田１丁目６番11号
(72)発明者　奥野　昌彦
東京都品川区東五反田１丁目６番11号

Ｆターム(参考)　5B085 AE26
5J104 AA07 KA01 KA17 KA18 KA19
MA01 NA05 NA27 NA35 NA41
NA43 PA10 PA11
5K027 AA11 BB09 EE11 FF01 FF22
HH11 HH20 HH23 MM03 MM17
5K067 AA32 BB04 DD17 DD51 EE02
EE10 HH23 HH24

(54)【発明の名称】　モバイル機器、モバイル機器の指紋認証方法及びモバイル機器の指紋認証プログラムを記録した記録媒体

(57)【要約】
【目的】　モバイル機器が使用者を知っており、本人確認が正確で、より一層の安全性が確保出来るモバイル機器を提供する。
【構成】　指紋データを記録する指紋記録媒体と、この指紋記録媒体から指紋データを読み出す指紋記録媒体リーダとを備えている。また指紋画像を読み込み指紋データを生成する指紋読取装置と、この指紋データを指紋認証サーバへ送信してこの指紋認証サーバによる本人確認の判定結果を受信する認証制御装置とを備えている。これ等により本人確認がされた場合にはモバイル機器としての各種動作を可能にする制御を行なう。また認証確認後に、受信した許可証やチケット等の認証データを、認証データ記録媒体を用いて記録して読み出す制御を行う。またＩＣカードが、指紋画像を読み込んで指紋データを生成する指紋読取装置を備えている。

【特許請求の範囲】

【請求項１】　指紋データを記録する指紋記録媒体と、この指紋記録媒体から指紋データを読み出す指紋記録媒体リーダとを備えていることを特徴とする、モバイル機器。

【請求項２】　指紋記録媒体部がモバイル機器に対して着脱自在に設けられている、請求項１に記載のモバイル機器。

【請求項３】　指紋記録媒体にデータを記録させるためのスイッチが設けられている、請求項１に記載のモバイル機器。

【請求項４】　更に新たに指紋画像を読み込んで指紋データを生成する指紋読取装置を備えている、請求項１に記載のモバイル機器。

【請求項５】　更に新たに指紋画像を読み込んで指紋データを生成する指紋読取装置と、この指紋データと前記指紋記録媒体リーダが読み出した指紋データとを比較して本人確認を行なう指紋データ比較装置と、これ等の認証制御装置とを備えている、請求項１に記載のモバイル機器。

【請求項６】　指紋画像を読み込み指紋データを生成する指紋読取装置と、この指紋データを指紋認証サーバへ送信してこの指紋認証サーバによる本人確認の判定結果を受信する認証制御装置とを備えていることを特徴とする、モバイル機器。

【請求項７】　指紋データの指紋認証サーバへの送信に公衆回線を利用するものである、請求項６に記載のモバイル機器。

【請求項８】　更に商店等に置かれた本人確認用のデータ端末に非接触にて指紋データを送信するための指紋データ送信装置を備えている、請求項１または請求項６に記載のモバイル機器。

【請求項９】　内部データを書換えるのに必要な書換データを受信するための書換データ受信装置を備えている、請求項１または請求項６に記載のモバイル機器。

【請求項１０】　受信した許可証やチケット等の認証データを記録して読み出すための認証データ記録媒体を備えている、請求項１または請求項６に記載のモバイル機器。

【請求項１１】　認証制御装置は本人確認が行なわれて初めてモバイル機器としての各種動作を可能にする制御を行なうものである、請求項５または請求項６に記載のモバイル機器。

【請求項１２】　指紋読取装置が筐体表側の情報表示窓に重ねて設けられている、請求項４または請求項５または請求項６に記載のモバイル機器。

【請求項１３】　指紋読取装置が筐体表側の情報表示窓以外の筐体部位に設けられている、請求項４または請求項５または請求項６に記載のモバイル機器。

【請求項１４】　指紋読取装置がスイッチ表面に設けられている、請求項４または請求項５または請求項６に記載のモバイル機器。

【請求項１５】　ＩＣカードが指紋画像を読み込んで指紋データを生成する指紋読取装置を備えていることを特徴とする、モバイル機器。

【請求項１６】　指紋記録媒体に予め記録された指紋データを、指紋記録媒体リーダを用いて読み出し、指紋読取装置によって新たに指紋画像を読み込んで指紋データを生成し、指紋データ比較装置によって前記指紋記録媒体リーダの指紋データと前記指紋読取装置の指紋データとを比較して本人確認を行ない、本人確認が為された場合にはモバイル機器としての各種動作を可能にする制御を行なうようにしたことを特徴とする、モバイル機器の指紋認証方法。

【請求項１７】　指紋読取装置により新たに指紋画像を読み込み指紋データを生成し、この指紋データを認証制御装置により指紋認証サーバへ送信してこの指紋認証サーバによる本人確認の判定結果を受信し、本人確認が為された場合には、モバイル機器としての各種動作を可能にする制御を行なうようにしたことを特徴とする、モバイル機器の指紋認証方法。

【請求項１８】　指紋データの指紋認証サーバへの送信に公衆回線を利用するものである、請求項１７に記載のモバイル機器の指紋認証方法。

【請求項１９】　商店等に置かれた本人確認用のデータ端末へ、非接触にて指紋データを送信するものである、請求項１７に記載のモバイル機器の指紋認証方法。

【請求項２０】　指紋読取装置によって新たに指紋画像を読み込んで生成した指紋データを、指紋認証サーバへ送信してこの指紋認証サーバによる本人確認の判定の結果を受信し、更に受信した許可証やチケット等の認証データを、認証データ記録媒体を用いて記録して読み出す、モバイル機器の指紋認証方法。

【請求項２１】　指紋記録媒体に予め記録された指紋データを読み出す指紋記録媒体リーダと、新たに指紋画像を読み込んで指紋データを生成する指紋読取装置と、を備えるモバイル機器のコンピュータに、本人確認を行なわせるためのプログラムを記録した記録媒体であって、指紋データ比較装置によって前記指紋記録媒体リーダの指紋データと前記指紋読取装置の指紋データとを比較して本人確認を行ない、本人確認が為された場合には、モバイル機器としての各種動作を可能にする制御を行なうことを特徴とする、モバイル機器の指紋認証プログラムを記録した記録媒体。

【請求項２２】　指紋記録媒体に予め記録された指紋データを読み出す指紋記録媒体リーダを備えるモバイル機器のコンピュータに、モバイル機器としての各種動作を可能にする制御プログラムを記録した記録媒体であって、指紋読取装置により新たに指紋画像を読み込み指紋データを生成し、この指紋データを認証制御装置により

指紋認証サーバへ送信して、この指紋認証サーバによる本人確認の判定結果を受信し、本人確認が為された場合には、モバイル機器としての各種動作を可能にする制御を行なうようにしたことを特徴とする、モバイル機器の指紋認証プログラムを記録した記録媒体。

【請求項２３】　指紋読取装置を備えるモバイル機器のコンピュータに本人確認を行なわせるためのプログラムを記録した記録媒体であって、指紋読取装置によって新たに指紋画像を読み込んで生成した指紋データを、指紋認証サーバへ送信してこの指紋認証サーバによる本人確認の判定結果を受信し、更に受信した許可証やチケット等の認証データを、認証データ記録媒体を用いて記録して読み出すようにしたことを特徴とする、モバイル機器の指紋認証プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、指紋データを取り扱うことが出来るようにしてより安全性が高く確実な本人確認を可能にするモバイル機器、モバイル機器の指紋認証方法、及びモバイル機器の指紋認証プログラムを記録した記録媒体に関するものである。

【０００２】

【従来の技術】従来の電子認証システムとしては、入力キーにより暗証番号を入力させ、その真偽を判定する暗証番号方式が一般的である。これは例えばクレジットカードやデビットカード等の磁気記録カード、またＩＣカードに代表されるような、認証トークンを使用する認証トークン方式と併用されることが多い。今後の動向として認証トークン方式には接触型或いは非接触型のＩＣカードが多用されるであろう。また場合によってはＩＣが埋め込まれた非接触型の指輪などのアクセサリーも使用されるであろう。これ等は内部に埋設したＩＣチップに本人確認のためのデータを納めたものである。

【０００３】またこれまではあまり一般的ではなかった電子認証システムとして、個人の身体的特性に着目するバイオメトリクス方式があった。これに付いては個人情報の取り扱いにより一層の安全性が求められると共に、例えば指紋読み取りのための装置自体の値段が低下して来ていることなどもあり、今後の動向としてはバイオメトリクス方式が多用されるようになるはずである。他者に管理されるのは嫌であるが、自分で管理出来るのであれば指紋を利用することも許容するというような認識になりつつある。

【０００４】このバイオメトリクス方式には、声紋認識、虹彩認識、指紋認識の各方式を上げることが出来る。声紋は声を周波数分析装置で複雑な縞模様に表わしたものでありこれを認証に用いることが出来る。虹彩は眼球の角膜と水晶体との間にあり中央に瞳孔をもつ円盤状の薄膜であり、括約筋や放射筋や色素の状態等によって個人を判別することが出来る。また指紋は指端の腹面にある皮膚のしわであり、弓状、渦状、蹄状を為し、人によって夫々異なり終生変らないため、個人識別の根拠として利用されている。

【０００５】これまで指紋識別装置の例としては、図２０で示すような光学センサを用いるもの、図２１で示すような静電容量方式による半導体センサを用いるものが知られている。光学識別機９は、ガラス９０面上に置かれた指に対して可視光や赤外線を放射する光源９１と、ガラス９０面で反射された光を受ける光学センサ９２と、この光学センサ９２とガラス９０面との間のフォーカル・プレーンに置かれるレンズ９３とを備える。光源９１としては発光ダイオードがよく用いられている。また光学センサ９２には電荷結合素子やイメージスキャナ等がよく用いられている。ガラス９０面上に現われる指紋はレンズ９３によりピントが合わされ、明暗の縞模様画像として光学センサ９２に拾われる。また静電容量識別機９４は指を置くピクセル・アレイ９５と指の縞模様凹凸（指紋）９６との間のキャパシタンスの分布の様子から縞模様画像を得るものであり、最近ではポインティングデバイスとしてのマウスの中央部分に半導体指紋センサを取り付けたものなどが登場して来ている。

【０００６】この指紋の映像信号はＡ／Ｄ変換部でデジタル信号の指紋データに変換され、マニューシャ方式やパターンマッチング方式などのよく知られた指紋識別処理に供される。また指紋識別装置の用途としては、上記マウスによるコンピュータへのログオンやインターネット通販の信用認証等、玄関やガレージのドアロックやアンロック、自動車のキーシステム等の個人使用的な分野での利用の他に、銀行の現金自動預け払い機、遊戯店に於ける会員認証システム、小売店での個人認証などのように、不特定多数の人々による共同利用を上げることが出来る。

【０００７】

【発明が解決しようとする課題】ところで、最近では携帯電話、ＰＨＳ、ＰＤＡ等々のモバイル機器が普及して来ている。しかしながら携帯電話やＰＨＳでは、紛失したりすると他人に使用される恐れがあり、この利用料は所有者が支払わなくては成らない。或いは紛失しないまでも子供には使わせたくないという場合もある。即ちモバイル機器が使用者を知っていなくては成らない。また携帯電話やＰＨＳやその他のモバイル機器から直接オンラインショッピングをすることが出来るように成って来たが、このセキュリティにも配慮する必要に迫られている。商店に於ける本人確認も重要である。この発明は上述したような問題を解決して、より一層の安全性が確保出来るモバイル機器を提供することを目的とする。

【０００８】

【課題を解決するための手段及び作用】このような問題を解決するものとして、当発明者は上述したバイオメトリクス方式による認証方法を採用すれば良いという知見

を得た。即ち上記課題は、指紋データを記録する指紋記録媒体と、この指紋記録媒体から指紋データを読み出す指紋記録媒体リーダと、を備えていることを特徴とするモバイル機器とすることにより達成される。モバイル機器が携帯電話やＰＨＳでは通話用やデータ通信用の送受信機を備えている。ＰＤＡや携帯型のパーソナルコンピュータ（ウェアラブルコンピュータなど）では送受信機を内蔵しているものと、後付けのものとがある。このモバイル機器はこのユーザーである本人の指紋データを、指紋記録媒体中に記録している。従って本人確認が必要な場合に、指紋記録媒体リーダを用いてこの指紋記録媒体から指紋データを読み出し、別途商店側の指紋読取装置によって新たに指紋画像を読み込んで指紋データを生成し、指紋データ比較装置によって両者を比較して本人確認を行なう、と言うようなことが出来る。

【０００９】また第１の手段に付き更に、指紋記録媒体部がモバイル機器に対して着脱自在に設けられているものとした。これは例えば指紋記録媒体部がＩＣカードであって、このＩＣカードが携帯電話やＰＨＳのカードスロットに着脱自在であることなどを言う。従って指紋記録媒体部を抜き出して保管したり、例えば商店との間で指紋データを交換する際などに指紋記録媒体部を抜き出して渡すことが出来るわけである。

【００１０】第１の手段に付き更に、指紋記録媒体にデータを記録させるためのスイッチが設けられているものとした。指紋記録媒体に本人データを後から本人が入力したいとする場合がある。このような時には前記スイッチを利用して入力することが出来る。スイッチとは、例えばモバイル機器が携帯電話やＰＨＳであれば、そのテンキーなどのことである。

【００１１】第１の手段に付き更に、新たに指紋画像を読み込み指紋データを生成する指紋読取装置を備えているものとした。従ってモバイル機器を指紋読取装置そのものとして使用することが出来、指紋データを自ら活用したり、他の装置へ渡すことが出来るように成る。またこの際、指紋記録媒体部の指紋データを使用することが出来る。即ち例えば自ら指紋を照合して本人確認を行なったり、２つのデータを他の装置へ渡すことが可能である。

【００１２】第１の手段に付き更に、新たに指紋画像を読み込み指紋データを生成する指紋読取装置と、この指紋データと前記指紋記録媒体リーダが読み出した指紋データとを比較して本人確認を行なう指紋データ比較装置と、これ等の認証制御装置とを備えているものとした。指紋記録媒体部に格納されている指紋データは本人のデータであるから、新たに読み込んだ指紋データとのマッチングが認証制御装置により取れていれば、この読み込んだ指紋は本人のものであると言うことが出来る。従って、モバイル機器を持っている者が本人であるか否かを、モバイル機器のみでチェックすることが可能と成る。而してこの結果を自ら活用したり、他の装置へ渡すことが出来る。

【００１３】次に、請求項６のモバイル機器は、指紋画像を読み込み指紋データを生成する指紋読取装置とこの指紋データを指紋認証サーバへ送信してこの指紋認証サーバによる本人確認の判定結果を受信する認証制御装置とを備えているものである。請求項５のモバイル機器と異なる点は指紋データを記録する指紋記録媒体を備えておらず、本人の指紋データを指紋認証サーバ側に置いておき、指紋読取装置により読み込まれて生成された指紋データを指紋認証サーバへ送信して認証させ、その結果を返して貰うようにした点に在る。従って指紋認証に付いては指紋認証サーバに任せることが出来るためその分シンプルな構成と成り、また指紋データを所有していないことから、それが読み出されて悪用されるなどの心配がない。なお、認証結果は自ら活用したり、他の装置へ渡すことが出来る。

【００１４】第６の手段に付き更に、指紋データの指紋認証サーバへの送信に、公衆回線を利用するものとした。モバイル機器が携帯電話やＰＨＳであれば通話用やデータ通信用の送受信機を備えているため、これを利用する。ＰＤＡや携帯型のパーソナルコンピュータでは携帯電話やＰＨＳを利用する。また後述するように、ＩＣカードはモバイル機器のカードスロットに挿入し、携帯電話やＰＨＳを送受信機として活用する。しかしながら公衆回線ではなく、赤外線や電波などを利用するようにすることも可能である。

【００１５】さて第１の手段または第６の手段に付き更に、商店等に置かれた本人確認用のデータ端末に非接触にて指紋データを送信するための指紋データ送信装置を備えているものとした。第１の手段は、記録された指紋データに関するものであり、第６の手段は、新たに読み込んだ指紋データに関するものであって、この何れも指紋データ送信装置によって商店等に置かれたデータ端末に指紋データを送信する。データ端末ではモバイル機器から受信した指紋データを、顧客の指紋データが保存された指紋サーバから所要の指紋データを取り寄せて比較照合を行なったり（データ端末が指紋認証サーバの役目を担う場合である）、モバイル機器から受信した指紋データを指紋認証サーバへ送信して本人確認して貰う場合の中継を行なう。

【００１６】また第１の手段または第６の手段に付き更に、モバイル機器は、内部データを書換えるのに必要な書換データを受信するための書換データ受信装置を備えているものとした。従って、例えば指紋照合すべき指を変更しなくては成らないような場合でも、書換データを受信して内部データを書換えることが出来る。

【００１７】また第１の手段または第６の手段に付き更に、モバイル機器は受信した許可証やチケット等の認証データを記録して読み出すための認証データ記録媒体を

備えているものとした。これは例えば、このモバイル機器を使用してオンライン店舗からコンサートチケットを購入するような場合、支払いを済ませる時にチケットを受信して認証データ記録媒体に記録し、コンサート会場の入口でこのモバイル機器より認証データを読み出して、正規の入場者であるか否かのチェックを行なうような場合に有効である。従って例えばチケットの購入や提示がこのモバイル機器だけで済むように成り、紙に印刷するチケットなども不要と成るなどの効果がある。

【００１８】次に第５の手段または第６の手段に付き更に、認証制御装置は本人確認が行なわれて初めてモバイル機器としての各種動作を可能にする制御を行なうものであるものとした。第５の手段は、前記指紋記録媒体リーダが読み出した指紋データと、指紋読取装置が新たに指紋画像を読み込んで生成した指紋データとを、自らの認証制御装置により比較して本人確認を行なうものであり、また第６の手段は指紋読取装置が新たに読み込んだ指紋データを、認証制御装置が指紋認証サーバへ送信しこの指紋認証サーバによる本人確認の判定結果を受信するものであり、この何れの場合も本人確認が行なわれて初めて、認証制御装置がモバイル機器としての各種動作を可能にする。従って例えば、自らの認証制御装置により比較して本人確認を行なうものでは、本人確認が為されるまでは通話が出来ないような携帯電話やＰＨＳを提供することが出来る。オンラインショッピング等に付いても同様に、本人確認が出来るまでは携帯電話やＰＨＳの使用を制限可能に設定すれば良い。また例えば指紋認証サーバによって本人確認を受けるものでは、通信装置部分は動作しているものの、本人確認が為されるまではコンピュータアプリケーションソフトウェアの使用を制限可能に設定すれば良い。

【００１９】また第４の手段または第５の手段または第６の手段に付き更に、指紋読取装置が筐体表側の情報表示窓に重ねて設けられているものとした。例えば液晶表示画面の情報表示窓の背後に指紋読取装置部を設けたものとするのである。この液晶表示画面は通常はモバイル機器のディスプレイとして各種表示が為されるわけであるが、この表示を消して透明にすることにより、指を置くための指紋認識窓として利用することが出来るように成る。このため液晶表示画面の内部には指紋読取装置部が設けられている。指紋読取装置部にはＣＣＤセンサや静電容量センサが利用される。従って例えば携帯電話やＰＨＳが電話機として使用出来ず、指紋読取装置部のみ動作している状態でこの指紋読取装置部に指先を当てさせて指紋データを取り、本人確認したならば電話機として使用出来るようにする、などの設定が可能と成る。

【００２０】また第４の手段または第５の手段または第６の手段に付き更に、指紋読取装置が筐体表側の情報表示窓以外の筐体部位に設けられているものとした。例えば、筐体裏側に指紋読取装置部を設けるなどである。従って、例えばモバイル機器が携帯電話やＰＨＳであれば、これを握ったまま人指し指を筐体裏側の指紋読取装置部に当てることが出来るように成る。

【００２１】また第４の手段または第５の手段または第６の手段に付き更に、指紋読取装置がスイッチ表面に設けられているものとした。モバイル機器には各種スイッチが設けられているが、この表面部で指紋を読み取ることが出来るようにするのである。スイッチにはＣＣＤセンサや静電容量センサが取り付けられる。従って指紋読取装置部がスイッチと兼用であるため、指紋読取装置部の設置場所を取らなくて済むという利点がある。

【００２２】次に、請求項１５のモバイル機器はＩＣカードに係り、ＩＣカードが指紋画像を読み込んで指紋データを生成する指紋読取装置を備えているものとした。ここではＩＣカードが指紋読取装置を備えているため、これもモバイル機器であると定義するものである。またＩＣカードは、他のモバイル機器例えばＰＤＡやパソコンのカードスロットに挿着して使用するが、指紋読取装置部を利用する場合にはカードスロットから取り出し、利用後には再びカードスロットに挿着するようにする。このようにしてＩＣカードは自己以外の他のモバイル機器に、読み取った指紋データを渡すのである。

【００２３】さて、請求項１６のモバイル機器の指紋認証方法は、指紋記録媒体に予め記録された指紋データを、指紋記録媒体リーダを用いて読み出し、指紋読取装置によって新たに指紋画像を読み込んで指紋データを生成し、指紋データ比較装置によって前記指紋記録媒体リーダの指紋データと前記指紋読取装置の指紋データとを比較して本人確認を行ない、本人確認が為された場合には、モバイル機器としての各種動作を可能にする制御を行なうようにしたことを特徴とするものである。これによってモバイル機器を持っている者が本人であるか否かを、モバイル機器のみでチェックすることが出来るように成り、本人である場合のみモバイル機器としての各種動作、即ち例えばＰＤＡならばオペレーティングシステムを起動する、と言うような制御が可能に成る。従って、他人に勝手にＰＤＡを使われてしまったり、プライベートなデータにアクセスされるような問題を防止することが出来る。

【００２４】次に、請求項１７のモバイル機器の指紋認証方法は、指紋読取装置により新たに指紋画像を読み込み指紋データを生成し、この指紋データを認証制御装置により指紋認証サーバへ送信してこの指紋認証サーバによる本人確認の判定結果を受信し、本人確認が為された場合には、モバイル機器としての各種動作を可能にする制御を行なうようにしたことを特徴とするものである。上述した請求項１６の指紋認証方法と異なる点は、比較すべき指紋データは指紋認証サーバが所有しており、モバイル機器から読み込んで生成した指紋データをこの指紋認証サーバへ送って本人確認をして貰い、確認が取れ

たならばモバイル機器としての各種動作を可能にしている点である。従って指紋認証に付いては指紋認証サーバに任せることが出来るためその分シンプルな構成と成り、また指紋データを所有していないことから、それが読み出されて悪用されるなどの心配がない。なお、認証結果は自ら活用したり、他の装置へ渡すことが出来る。例えば請求項２０の発明の項で述べるように認証データ記録媒体を用い、指紋認証サーバから受信した許可証やチケット等の認証データを記録して読み出すなどである。

【００２５】また第１７の手段に付き更に、指紋データの指紋認証サーバへの送信には公衆回線を利用する方法とした。モバイル機器が携帯電話やＰＨＳであれば通話用やデータ通信用の送受信機を備えているため、これを利用する。ＰＤＡや携帯型のパーソナルコンピュータでは携帯電話やＰＨＳを利用する。また後述するようにＩＣカードはモバイル機器のカードスロットに挿入し、携帯電話やＰＨＳを送受信機として活用する。しかしながら公衆回線ではなく、赤外線や電波などを利用するようにすることも可能である。このように公衆回線を利用する送受信機部分だけは動作可能でなくては成らない。

【００２６】また第１７の手段に付き更に、商店等に置かれた本人確認用のデータ端末へ、非接触にて指紋データを送信するものである方法とした。例えば商店店頭に置かれたデータ端末上に、携帯電話、ＰＨＳ、ＰＤＡ、ＩＣカード等のモバイル機器を載せるようにすると、これ等のモバイル機器から受信した指紋データを、このデータ端末は、顧客の指紋データが保存された指紋サーバから所要の指紋データを取り寄せて比較照合を行なったり、或いは指紋認証サーバへ送信して本人確認して貰う場合の中継を行なったりするのである。

【００２７】次に請求項２０のモバイル機器の指紋認証方法は、指紋読取装置によって新たに指紋画像を読み込んで生成した指紋データを、指紋認証サーバへ送信してこの指紋認証サーバによる本人確認の判定の結果を受信し、更に受信した許可証やチケット等の認証データを、認証データ記録媒体を用いて記録して読み出すようにしたことを特徴とするものである。本人確認が出来さえすれば、モバイル機器は許可証やチケット等の認証データを受け取ることが出来るようにする。またこの認証データを例えばコンサート会場で読み出して提示することが出来る。従って携帯電話やＰＨＳはこの目的に最適である。

【００２８】次に請求項２１のモバイル機器の指紋認証プログラムを記録した記録媒体は、指紋記録媒体に予め記録された指紋データを読み出す指紋記録媒体リーダと、新たに指紋画像を読み込んで指紋データを生成する指紋読取装置と、を備えるモバイル機器のコンピュータに本人確認を行なわせるための、プログラムを記録した記録媒体であって、指紋データ比較装置によって前記指紋記録媒体リーダの指紋データと前記指紋読取装置の指紋データとを比較して本人確認を行ない、本人確認が為された場合には、モバイル機器としての各種動作を可能にする制御を行なうことを特徴とするものである。このプログラムによれば、コンピュータにモバイル機器の正当なユーザーであるか否かを確認させ、正当なユーザーであることが確認された場合には、例えば携帯電話やＰＨＳを電話機として使用可能にするなどの制御を行なうことが出来る。

【００２９】また請求項２２のモバイル機器の指紋認証プログラムを記録した記録媒体は、指紋記録媒体に予め記録された指紋データを読み出す指紋記録媒体リーダ備えるモバイル機器のコンピュータに、モバイル機器としての各種動作を可能にする制御プログラムを記録した記録媒体であって、指紋読取装置により新たに指紋画像を読み込み指紋データを生成し、この指紋データを認証制御装置により指紋認証サーバへ送信して、この指紋認証サーバによる本人確認の判定結果を受信し、本人確認が為された場合には、モバイル機器としての各種動作を可能にする制御を行なうようにしたことを特徴とするものである。即ち、指紋データの比較を指紋認証サーバに任せるようにしている。このプログラムによれば、指紋認証サーバとの通信によってモバイル機器の正当なユーザーであるか否かを確認し、正当なユーザーであることが確認された場合には、例えば携帯電話やＰＨＳを電話機として使用可能にするなどの制御を行なう。

【００３０】また請求項２３のモバイル機器の指紋認証プログラムを記録した記録媒体は、指紋読取装置を備えるモバイル機器のコンピュータに本人確認を行なわせるためのプログラムを記録した記録媒体であって、指紋読取装置によって新たに指紋画像を読み込んで生成した指紋データを、指紋認証サーバへ送信してこの指紋認証サーバによる本人確認の判定結果を受信し、更に受信した許可証やチケット等の認証データを、認証データ記録媒体を用いて記録して読み出すようにしたことを特徴とする。携帯電話やＰＨＳでは通話用やデータ通信用の送受信機を備えているため、これを活用して指紋データを交換したり、チケット等の購入を行なうことが出来る。しかもチケット等は紙媒体を必要としない点で、環境的にも優れたものであると言うことが出来る。

【００３１】なおこの発明に於いてモバイル機器と、商店等に置かれた本人確認用のデータ端末と、指紋認証センターの指紋認証サーバとの連係は、今後の主流のひとつと成るであろう。またここにクレジットカード会社が参加するであろう。モバイル機器が携帯電話やＰＨＳであれば、クレジットカード会社ではなくこの電話会社が決済手段を提供するであろう。またこれ等が指紋認証サーバを管理する形態も在り得る。上述した非接触型の通信システムとしてはブルートゥース（商標）等が有名である。なお上記各請求項では指紋認証を取り扱っている

が、声紋や虹彩等のバイオメトリックスに差し替えることも可能である。この場合指紋記録媒体を声紋記録媒体と書き換え指紋記録媒体リーダを虹彩記録媒体リーダと書き換えれば良いだけであり、設計変更も容易であるため、これ等もまたこの発明の権利範囲内にある。

【００３２】

【発明の実施の形態】以下、この発明の幾つかの実施形態を図面に基づいて説明するが、この発明はこれ等の実施形態にのみ限定されるものではない。

【００３３】第１実施形態

図１及び図２は第１実施形態の携帯型電話機２を表わしたものである。これは液晶表示画面２０を備えており、内部的には指紋データを記録する指紋記録媒体１０と、この指紋記録媒体１０から指紋データを読み出す指紋記録媒体リーダである制御部１と、通話用及びデータ通信用の通信部１１とを備えている。指紋記録媒体１０はこのユーザーである本人の指紋データを記録している。この実施形態によれば、指紋記録媒体１０から指紋データを呼び出すと、外部の機器例えば商店側の指紋読取装置などと連係するために、指紋データを通信部１１を利用して送り出すように成っている。

【００３４】第２実施形態

図３及び図４は第２実施形態の携帯型電話機２を表わしたものである。上述した第１実施形態のものに加えて、ダイアル用のスイッチ２１により指紋記録媒体１０に対して新たなデータを記録させることが出来るものである。新たなデータとは変更されたパスワードであったり、通信部１１を介して導入するユーザーの別の指の指紋データであったりする。従って、スイッチ２１はパスワードを入力したり、制御部１を操作するためのものである。なおこの実施形態では指紋記録媒体１０をカード型にして携帯型電話機２に対し着脱自在とした。これによってユーザー毎に指紋記録媒体１０を所有すれば、携帯型電話機２を共用とすることも可能と成る。

【００３５】第３実施形態

図５乃至図７は第３実施形態の携帯型電話機２を表わしたものである。ここで符号２２は液晶表示画面兼用の半導体指紋センサであり、この上に指を置くことにより指紋データを取ることが出来る。制御部１は指紋データ照合部１４を制御しており、指紋データ照合部１４は指紋記録媒体１０から読み出した指紋データと指紋読取部１３から得られた指紋データとを照合する。まず指紋記録媒体１０から指紋データを読み出してバッファ１に記憶する（ステップＳ１）。次に液晶表示画面上の半導体指紋センサ２２から新たに指紋を読み取りバッファ２に記憶する（ステップＳ２）。そして指紋データ照合部１４がバッファ１とバッファ２の指紋データを照合し（ステップＳ３）、マッチしていればＯＫを、マッチしていなければＮＧを発する。ここでは半導体指紋センサ２２から新たに読み取った指紋データを指紋データ照合部と言う自らの目的のために使用しているが、他の装置へ渡すことも可能である。

【００３６】第４実施形態

図８乃至図１０は第４実施形態の携帯型電話機２を表わしたものである。この実施形態の携帯型電話機２が第１実施形態のものと異なる点は指紋記録媒体１０の代わりに指紋読取部１３を備えている点に在る。制御部１は指紋読取部１３で読み取った指紋データを（ステップＳ４）、通信部１１を介して、図９で表わした認証サーバ３へ送信し（ステップＳ５）、認証サーバ３からの認証結果を受信する（ステップＳ６）。上述したように通信部１１は、携帯型電話機２の通話用及びデータ通信用のものを利用している。また指紋読取部１３は液晶表示画面上の半導体指紋センサ２２を利用したものである。

【００３７】なお、この携帯型電話機２には映像を伴なった通話が可能と成るようにカメラ２３を備えているが、半導体指紋センサ２２による指紋認識ではなくて、カメラ２３による虹彩認識を行なうように設計することが可能である。また通話用としてマイク２４を備えているが、これを利用して声紋認識を行なうように設計することも出来る。

【００３８】なお、認証サーバ３はインターネットに接続されている。またインターネットには商店に置かれたＩＣカードリーダ４が接続されている。ＩＣカードリーダ４は、カード挿入溝４０とモバイル機器載置部４１とを備えている。カード挿入溝４０に指紋記録媒体１０（ここではＩＣカードである）を差し込んでスライドさせると、内蔵された制御部は非接触状態のまま指紋記録媒体１０内に記録されている本人確認用のデータを読み出す。或いはまた、上述した非接触型の通信システムとしてのブルートゥース（商標）チップが内蔵されたＰＨＳ等々のモバイル機器であれば、それをこのモバイル機器載置部４１上に載置するだけでこのＩＣカードリーダ４と通信することが出来る。ＩＣカードリーダ４はインターネットを介して認証サーバ３に本人確認を依頼する。

【００３９】第５実施形態

図１１は第５実施形態の携帯型電話機をブロック図にて表わしたものである。この携帯型電話機の制御装置１は、指紋読取部１３で読み取った指紋データを、通信部１５を介して、上述した商店に置かれたＩＣカードリーダ４へ送ることが出来るように設計されている。通信部１５は携帯型電話機２の通話用及びデータ通信用のものとは別個に設けられた、ＩＣカードリーダ４のモバイル機器載置部４１の送受信部（図示せず）との間で、無線でデータの送受を行なうデバイスである。

【００４０】第６実施形態

図１２は第６実施形態の携帯型電話機をブロック図にて表わしたものである。指紋データを記録する指紋記録媒体１０と、指紋記録媒体１０から指紋データを読み出す

指紋記録媒体リーダである制御部１と、通話用及びデータ通信用の通信部１１と、書換データ記録媒体１６とを備えている。既に説明したように、指紋記録媒体１０にはこのユーザーである本人の指紋データが記録されている。この実施形態によれば、指紋記録媒体１０から指紋データを呼び出すと、外部の機器例えば商店側の指紋読取装置などと連係するために、指紋データを通信部１１を利用して送り出すように成っている。更に制御部１は、書換データ受信装置としての通信部１１と書換データ記録媒体１６とを活用し、例えば指紋照合すべき指を変更するための指紋データとパスワードを受信して、新しい指紋データで指紋記録媒体１０に上書きすると共に、書換データ記録媒体１６へは新規パスワードと変更情報とを記憶させる。

【００４１】第７実施形態

図１３は第７実施形態の携帯型電話機をブロック図にて表わしたものである。指紋データを記録する指紋記録媒体１０と、指紋記録媒体１０から指紋データを読み出す指紋記録媒体リーダである制御部１と、通話用及びデータ通信用の通信部１１と、認証データ記録媒体１７とを備えている。認証データ記録媒体１７には、購入したチケットや、通行証などを記録することが出来る。従って常の如く本人確認が為されたならば、即ち正当に課金することが可能であれば、販売者側ではチケットを販売して料金を引き落とすことが出来るわけであり、チケットは通信部１１を介して認証データ記録媒体１７に記録されることに成る。最終的にはチケットを提示する場面で、制御部１は認証データ記録媒体１７からチケットデータを読み出し、携帯型電話機の図示していない液晶表示画面に表示したり、通信部１１を介して相手の認証機器へ送信するようにすれば良い。

【００４２】第８実施形態

図１４は第８実施形態をフローチャートで表わしたものである。この実施形態の目的は、指紋を登録した本人以外の者には、携帯電話等のモバイル機器を使用させないようにすることにある。モバイル機器は２つのスイッチを備えている。一般的な電源スイッチと、指紋認証用のスイッチとである。初めに指紋認証用のスイッチをＯＮ状態にする（ステップＳ７）。この状態では電源スイッチをＯＮ状態にすることは未だ出来ない。次に新たに指紋を読み取り（ステップＳ８）、予め内部の指紋記録媒体に記録されている指紋を読み出して（ステップＳ９）、両者を照合し（ステップＳ１０）、認証されたならば、電源スイッチを自動的にＯＮ状態にするが（ステップＳ１１）、認証されなかった場合にはＮＧであるとして電源スイッチをＯＦＦ状態のままに保つ。従って、予め指紋記録媒体に登録したユーザーしかこのモバイル機器を使用することが出来ない。なおスイッチを２種にせず電源スイッチは入るようにするも、認証されなかった場合にダイアル出来ないなどの制御を行なうように設計しても良い。

【００４３】第９実施形態

図１５は第９実施形態を背面外観図で表わしたものである。半導体指紋センサ２５をＰＨＳの裏側に設けると共に、指紋読み取りとそれに続く認証作業を開始するためのスイッチ２６を設けて成る。なおこのスイッチ２６はスライドさせてロックを解除すると押圧可能と成るものである。

【００４４】第１０実施形態

図１６は第１０実施形態を正面外観図で表わしたものである。符号２０は液晶表示画面であるが、この下側中央部に半導体指紋センサ２７を設けて成る。この上に人指し指などの指の腹を当着するようにして指紋の読み取りを行なう。なお図１７で示すように、半導体指紋センサ２７の裏側には液晶表示画面２８が重合されており、普段はここに表示が見られるように成っている。

【００４５】第１１実施形態

図１８は、この実施形態のＩＣカード５である。このＩＣカード５には半導体指紋センサ５０とスイッチ５１とが設けられている。また図示しないが、内部的には指紋記録領域が設定されており、半導体指紋センサ５０で読み取られた指紋データはここに記録される。而して、このモバイル機器としてのＩＣカード５が他のモバイル機器例えば携帯型パーソナルコンピュータ、携帯電話などのカードスロットに挿着され、或いは商店のＩＣカードリーダやキオスク端末等のカードスロットに挿着されて、指紋記録領域の指紋データが読み出される。

【００４６】第１２実施形態

図１９は第１２実施形態のフローチャートであり、この携帯型電話機は、指紋読取装置で読み取った指紋データを通話用及びデータ通信用の通信部を利用して指紋認証サーバへ送る。次にこの指紋認証サーバの認証の結果、本人確認が為されていれば、チケットなどの電子データの購入が可能と成っているため、ここでチケットを購入する手続きを行ない、決済に許可を与え、認証データ記録媒体にチケットなどの電子データをダウンロードする。

【００４７】なお、モバイル機器のコンピュータに本人確認を行なわせるためのプログラムを記録した記録媒体には、メモリカード（上述したＩＣカードも含む）、ＣＤ－ＲＯＭ、ハードディスク、フレキシブルディスク、ＲＯＭ、ＲＡＭ等を含んでいる。

【００４８】またこの発明は上述した実施形態に限定されないから、今後登場するであろう各種のモバイル機器、例えばウェアラブルコンピュータ、時計型デバイス、人体埋込型デバイスなどに適用可能である。また指紋は複数種類を記録しておいたり複数種類を読み取れるようにしても良い。これ等は任意設計事項である。

【００４９】

【発明の効果】以上この発明は、指紋データを記録する

指紋記録媒体と、この指紋記録媒体から指紋データを読み出す指紋記録媒体リーダとを備えているモバイル機器、また指紋画像を読み込み指紋データを生成する指紋読取装置と、この指紋データを指紋認証サーバへ送信してこの指紋認証サーバによる本人確認の判定結果を受信する認証制御装置とを備えているモバイル機器、またＩＣカードが指紋画像を読み込んで指紋データを生成する指紋読取装置を備えているもの、またそれ等に係わるモバイル機器の指紋認証方法、またモバイル機器の指紋認証プログラムを記録した記録媒体に関するものとした。

【００５０】このように、指紋などのバイオメトリクスをモバイル機器に適用することで、より一層の安全性を備えたモバイル機器を提供することに成功し、所期の目的を達成することが出来た。

【図面の簡単な説明】

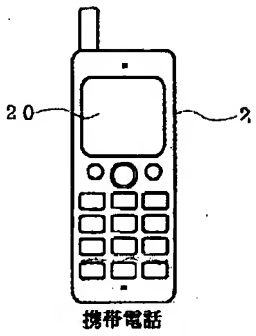
【図１】第１実施形態のブロック図である。
【図２】同実施形態の外観図である。
【図３】第２実施形態のブロック図である。
【図４】同実施形態の外観図である。
【図５】第３実施形態の外観図である。
【図６】同実施形態のブロック図である。
【図７】同実施形態のフローチャートである。
【図８】第４実施形態のブロック図である。
【図９】同実施形態のネットワーク図である。
【図１０】同実施形態のフローチャートである。
【図１１】第５実施形態のブロック図である。
【図１２】第６実施形態のブロック図である。
【図１３】第７実施形態のブロック図である。
【図１４】第８実施形態のフローチャートである。
【図１５】第９実施形態の外観図である。
【図１６】第１０実施形態の外観図である。
【図１７】同実施形態の模式図である。
【図１８】第１１実施形態の外観図である。
【図１９】第１２実施形態のフローチャートである。
【図２０】光学センサ９２を用いた従来例の模式図である。
【図２１】静電容量方式による半導体センサ９５を用いた従来例の模式図である。

【符号の説明】

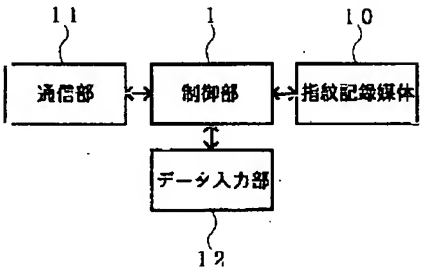
１　制御部
１０　指紋記録媒体
１１　通信部
１２　データ入力部
１３　指紋読取部
１４　指紋データ照合部
１５　通信部
１６　書換データ記録媒体
１７　認証データ記録媒体
２　携帯型電話機
２０　液晶表示画面
２１　スイッチ
２２　半導体指紋センサ
２３　カメラ
２４　マイク
２５　半導体指紋センサ
２６　スイッチ
２７　半導体指紋センサ
２８　液晶表示画面
３　認証サーバ
４　ＩＣカードリーダ
４０　カード挿入溝
４１　モバイル機器載置部
５　ＩＣカード
５０　半導体指紋センサ
５１　スイッチ

【図1】

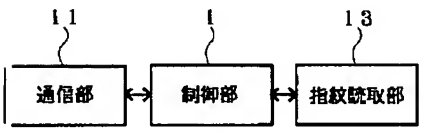
【図2】



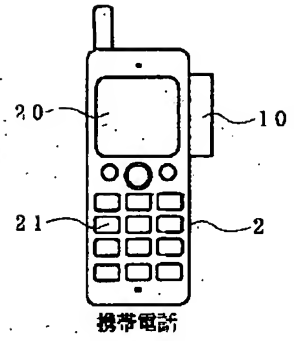
【図3】



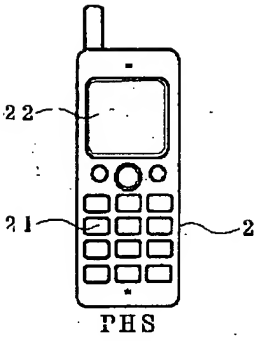
【図8】



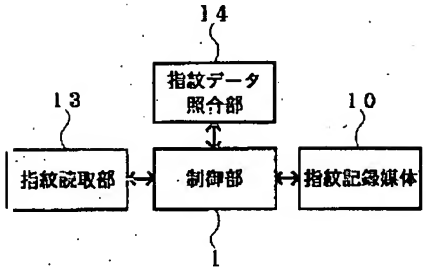
【図4】



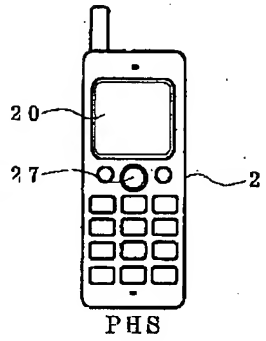
【図5】



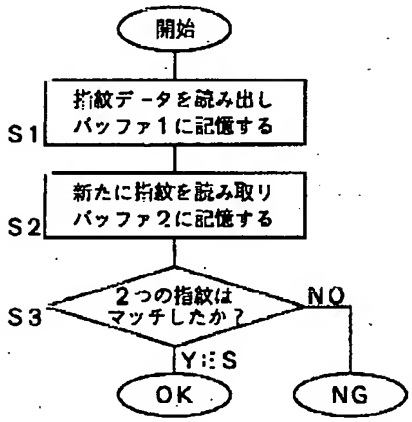
【図6】



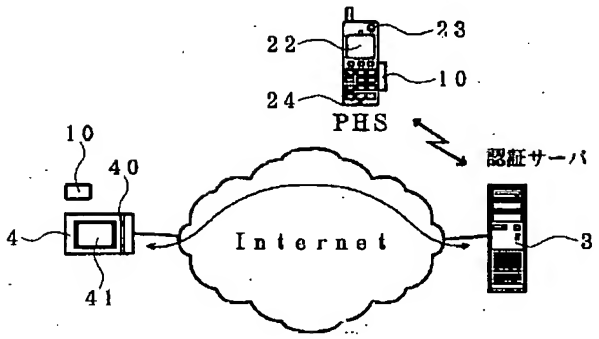
【図16】



【図7】

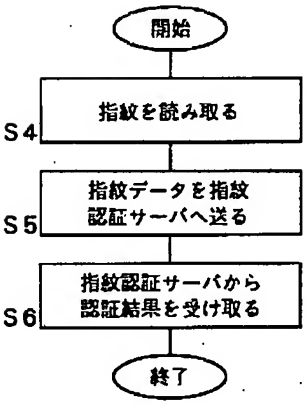


【図9】



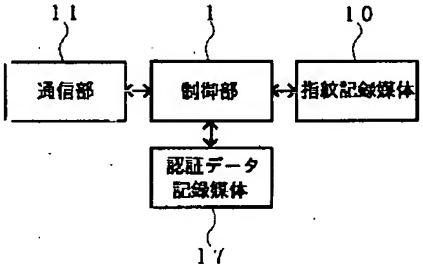
【図12】

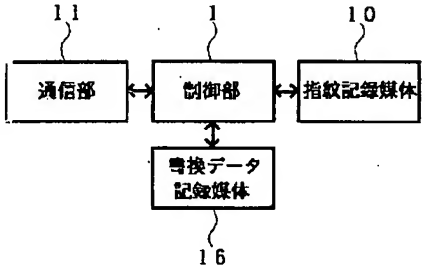
【図10】



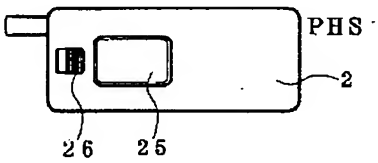
【図11】

【図13】

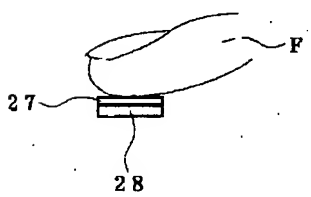




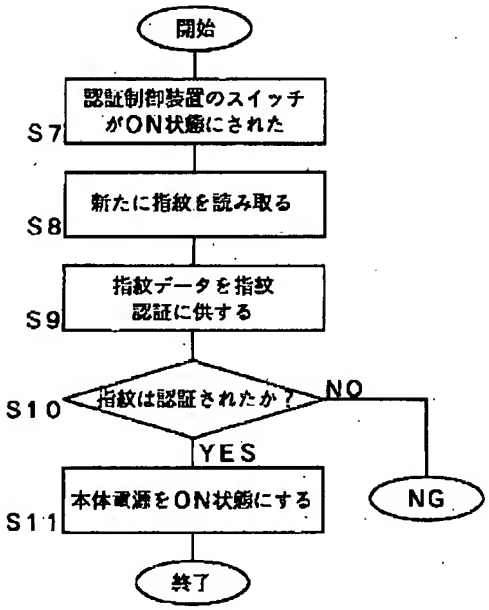
【図15】



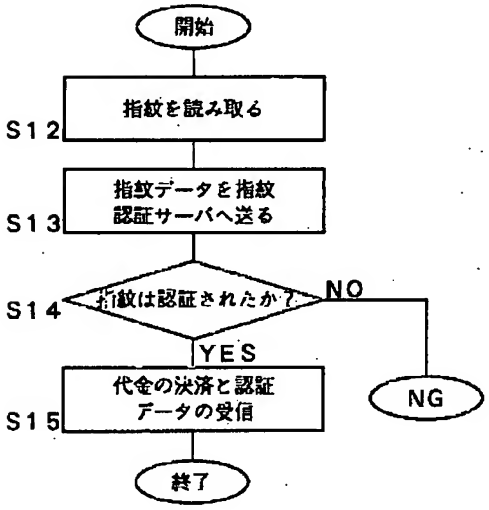
【図17】



【図14】

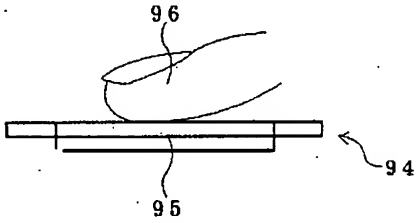


【図19】

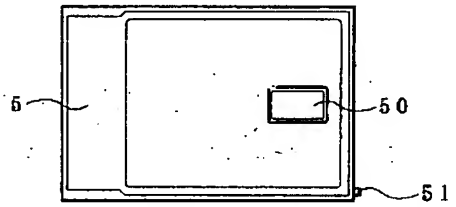


【図21】

従来例

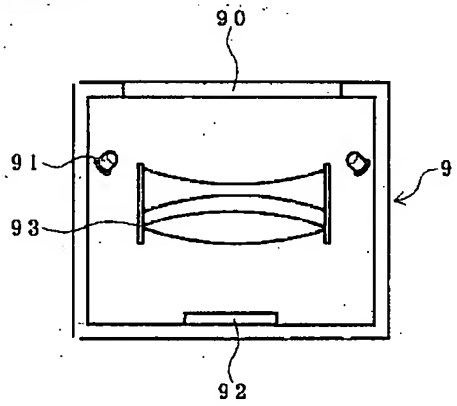


【図18】



【図20】

従来例



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		(参考)
H04L 9/32		H04L 9/00	673A	
			673D	
			673E	
			675D	